REMARKS

Favorable reconsideration of this application is respectfully requested in view of the foregoing amendments and the following remarks.

No claims have been canceled or added by this response. Claims 1, 3, 5, 8, 13, 15, 16, 18, 22-25, 27, 28, 34 and 35 have been amended. Thus, claims 1, 3-5, 8, 13, 15-18, 22-25, 27, 28, 34, 35, 41 and 43 are pending in the present application, of which claims 1, 3, 5, 8, 13, 15, 16, 18, 22-25, 27, 28, 34 and 35 are independent.

Noted - Priority Document Received By USPTO

The indication (see the Summary page of the Office Action mailed on May 11, 2007, boxes 12(a) as checked) that the certified copy(ies) of the priority document(s) has been received by the USPTO is noted with appreciation.

Noted - IDS Considered

The indication (see Examiner-initialed for PTO-1449 mailed with the Office Action mailed on May 11, 2007, January 11, 2008, June 15, 2009 and January 21, 2010) that the Information Disclosure Statement (IDS) as filed on March 30, 2004, April 18, 2007, August 7, 2007, January 6, 2009, February 18, 2009, March 9, 2009, September 2, 2009, October 13, 2009 and December 15, 2009 and references listed therein have been considered is noted with appreciation.

Noted - Drawings Approved

The indication (see the Summary page of the Office Action mailed on May 11, 2007, boxes 10(a) are checked) that the Drawings (submitted on March 30, 2004) have been approved is noted with appreciation.

Claim Rejections Under 35 U.S.C. §112

Claims 1, 3, 5, 8, 13, 15, 16, 22-25, 27 and 28 are rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement.

First, claim 1 amended in the last Response included the following limitation:

> changing the measurement parameters when the communication is judged to have been executed by the worm at the judging,
>
> wherein the acquiring includes acquiring, based on the measurement parameters changed at the changing, the information on the communication judged to have been executed by the worm at the judging

The above limitation is supported by the Specification at page 9, line 23 to page 10, line 5 or at page 38, line 19 to page 39, line 15.

Similar arguments to above also apply to claims 13 and 15.

Second, as to "measurement parameters", by the foregoing amendments, the claims have been amended to comply with the written description requirement.

Third, the Office Action states that there is no disclosure for the amended limitation: "all three conditions are satisfied" recited in claims 5 and 18, and that there is no disclosure for this claim limitation in the specification or the original claims.

However, in the Response for the Office Action dated January 11, 2008, claims 5 and 18 were amended to include the limitation included in claims 4 and 17, respectively. And claims 5 and 18, prior to being amended in the last Response, already included the "three conditions", namely:

> (1) a communication from the computer in the predetermined network segment is judged to be infected by the worm at the first judging
>
> (2) there is an increase in number of communication packets that are transmitted from the predetermined network segment to the outside
>
> (3) a number of destination addresses of the communication packets that are transmitted from the predetermined network segment

to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging.

The following shows the amendments to claim 5 in the last Response.

... wherein

the second judging includes judging that a plurality of computers in the predetermined network segment are infected by the worm when all three conditions are satisfied, the three conditions being that

a communication from the computer in the predetermined network segment is judged to be infected by the worm at the first judging,

~~there is an increase in~~ a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging, and

a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging

Further, the Specification supports the above limitation at page 25, line 24 to page 28, line 7.

Arguments similar to above also apply to claim 18.

Accordingly, withdrawal of the rejection is respectfully requested.

Claim Rejection Under 35 U.S.C. §103

Claims 1, 3-5, 8, 13, 15-18, 22-24, 34, 41 and 43 are rejected under 35 U.S.C. §103(a) as being unpatentable over Spiegel et al. (US Patent No. 7,159,149, hereinafter

Spiegel) in view of Willebeek-LeMair et al. (US Publication No. 20030204632, hereinafter Willebeek-LeMair).

Claims 25, 27, 28 and 35 are rejected under 35 U.S.C. §103(a) as being unpatentable over Spiegel in view of Willebeek-LeMair and further in view of Bunker et al. (US Publication No. 20030056116, hereinafter Bunker).

INDEPENDENT CLAIMS 1 AND 13

As an example, independent claims 1 and 13 each recite (among other things) the following features:

> acquiring information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on first setting information for a plurality of setting items;
>
> ...
>
> wherein the acquiring includes acquiring information of the monitored communication, based on second setting information for the plurality of setting items after the monitored communication is judged to have been executed by the worm at the judging.

As will be explained below, at least the above-noted features of claims 1 and 13 are a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses, at column 5, lines 15-21, column 5, lines 47-53, column 6, lines 15-26 and column 5, lines 38-42, "... This technique allows for the threshold criteria to be dynamic, adapting to the particular operating environment of each system", "... the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address. ...", "... an embodiment of the WDS 100 ..." and "... these thresholds can be easily reconfigured to catch new breeds of worms. ... a parameter that can be set depending on the system requirements", respectively.

However, Spiegel fails to disclose or suggest:

> acquiring information of a monitored communication, ..., based on first setting information for a plurality of setting items;
>
> ...
>
> ... acquiring information of the monitored communication, based on second setting information for the plurality of setting items after the monitored communication is judged to have been executed by the worm at the judging.

(underlining added for emphasis)

Willebeek-LeMair discloses the following at paragraph [0056].

> the agent 126 operates to assess changes to the network 14 detected by the network discovery functionality 112, confirm their validity, and inform the intrusion detector functionality 116 to tune its operation so that false alerts are not generated when the new, but nonetheless valid, information types are encountered in the network traffic content.

In the above disclosure, tuning "its operation" is performed for "when the new, but nonetheless valid, information types are encountered in the network traffic content", but not for "the monitored communication" that is "judged to have been executed by the worm", as recited in claims 1 and 13.

Hence, the above-noted features of claims 1 and 13 are a distinction over Spiegel and also Willebeek-LeMair.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claims 1 and 13 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claims 1 and 13. Claim 4 depends from claim 1, and so at least similarly distinguishes over the asserted combination of references.

INDEPENDENT CLAIM 15

As an example, independent claim 15 recites (among other things) the following features:

> an acquiring unit that acquires information of a monitored communication, the information being related to a traffic and a communication address of a communication packet, based on first setting information for a plurality of setting items;
>
> ..., wherein
>
> the acquiring unit acquires information of the monitored communication, based on second setting information for the plurality of setting items after the monitored communication is judged to have been executed by the worm by the judging unit.

As will be explained below, at least the above-noted features of claim 15 are a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses, at column 5, lines 15-21, column 5, lines 47-53, column 6, lines 15-26 and column 5, lines 38-42, "... This technique allows for the threshold criteria to be dynamic, adapting to the particular operating environment of each system", "... the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address. ...", "... an embodiment of the WDS 100 ..." and "... these thresholds can be easily reconfigured to catch new breeds of worms. ... a parameter that can be set depending on the system requirements", respectively.

However, Spiegel fails to disclose or suggest:

> an acquiring unit that acquires information of a monitored communication, ..., based on <u>first setting information</u> for a plurality of setting items;
>
> ..., wherein
>
> the acquiring unit acquires information of <u>the monitored communication</u>, based on <u>second setting information</u> for the plurality of setting items after the monitored communication is judged to have been executed by the worm by the judging unit.

(<u>underlining</u> added for emphasis)

Willebeek-LeMair discloses the following at paragraph [0056].

> the agent 126 operates to assess changes to the network 14 detected by the network discovery functionality 112, confirm their validity, and inform the intrusion detector functionality 116 to tune its operation so that false alerts are not generated when the new, but nonetheless valid, information types are encountered in the network traffic content.

In the above disclosure, tuning "its operation" is performed for "when the new, but nonetheless valid, information types are encountered in the network traffic content", but not for "the monitored communication" that is "judged to have been executed by the worm", as recited in claim 15.

Hence, the above-noted features of claim 15 are a distinction over Spiegel and also Willebeek-LeMair.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 15 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 15. Claim 17 depends from claim 15, and so at least similarly distinguishes over the asserted combination of references.

INDEPENDENT CLAIM 3

As an example, independent claim 3 recites (among other things) the following features:

> judging whether the monitored communication has been executed by the worm based on the information acquired and a first predetermined judgment criteria;
>
> ..., wherein
>
> the judging includes further judging whether the monitored communication has been executed by the worm after the monitored communication is judged to have been executed by the worm at the

> judging, based on the information acquired and a second predetermined judgment criteria.

As will be explained below, at least the above-noted features of claim 3 are a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses at column 5, lines 8-10, column 5, lines 15-21 and column 6, lines 15-22, "... the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time. ...", "... This technique allows for the threshold criteria to be dynamic, adapting to the particular operating environment of each system" and "... an embodiment of the WDS 100 ...", respectively.

However, Spiegel fails to disclose or suggest:

> judging whether the monitored communication has been executed by the worm based on the information acquired and a first predetermined judgment criteria;
>
> ...,
>
> ... further judging whether the monitored communication has been executed by the worm after the monitored communication is judged to have been executed by the worm at the judging, based on the information acquired and a second predetermined judgment criteria.

(underlining added for emphasis)

Hence, the above-noted features of claim 3 are a distinction over Spiegel. The noted features also are a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted features.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 3 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 3. Claim

41 depends from claim 3, and so at least similarly distinguishes over the asserted combination of references.

INDEPENDENT CLAIM 16

As an example, independent claim 16 recites (among other things) the following features:

> a judging unit that judges whether the monitored communication has been executed by the worm based on the information acquired and a first predetermined judgment criteria;
>
> ..., wherein
>
> the judging unit further judges whether the monitored communication has been executed by the worm after the monitored communication is judged to have been executed by the worm by the judging unit, based on the information acquired by the acquiring unit and a second predetermined judgment criteria.

As will be explained below, at least the above-noted features of claim 16 are a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses at column 5, lines 8-10, column 5, lines 15-21 and column 6, lines 15-22, "... the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time. ...", "... This technique allows for the threshold criteria to be dynamic, adapting to the particular operating environment of each system" and "... an embodiment of the WDS 100 ...", respectively.

However, Spiegel fails to disclose or suggest:

> a judging unit that judges whether the monitored communication has been executed by the worm based on the information acquired and <u>a first predetermined judgment criteria</u>;
>
> ..., wherein
>
> the judging unit further judges whether <u>the monitored communication</u> has been executed by the worm after the monitored communication is judged to have been executed by the worm by the judging unit, based on the information acquired by the acquiring unit and <u>a second predetermined judgment criteria</u>.

(<u>underlining</u> added for emphasis)

Hence, the above-noted features of claim 16 are a distinction over Spiegel. The noted features also are a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted features.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 16 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 16.

INDEPENDENT CLAIM 5

As an example, independent claim 5 recites (among other things) the following features:

> the second judging includes judging that a plurality of computers in the predetermined network segment are infected by the worm when all three conditions are satisfied, the three conditions being that
>
> a monitored communication from the computer in the predetermined network segment is judged to be infected by the worm at the first judging,
>
> a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging, and
>
> a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging

As will be explained below, at least the above-noted features of claim 5 are a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses at column 5, lines 8-10, column 5, lines 47-50, column 6, lines 15-22 and column 3, lines 20-27, "... the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time. ...", "... the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address. ...", "... an embodiment of the WDS 100 ..." and "... If infected, a process 20 is likely to produce a relatively large number of connection attempts to remote destination addresses over a given period of time. ...", respectively.

Spiegel also discloses at column 1, lines 50-60, column 1, lines 60-67, column 3, line 63 to column 4, line 9, "... a network monitoring module (110) observes (205) failed network connection attempts from multiple sources (10,20). ...", "... this determination is based on a set of threshold criteria. ..." and the following, respectively.

> ... the threshold criteria include any one or a combination of the following metrics: (1) the number of failed network connection attempts; (2) the diversity of destination network addresses associated with the failed network connection attempts; (3) the randomness of the failed addresses; and (4) a weighting for each failed network connection attempt according to an attribute thereof (e.g., source or destination address)

However, Spiegel fails to disclose or suggest the following:

> the second judging includes judging that a plurality of computers in the predetermined network segment are infected by the worm <u>when all three conditions are satisfied</u>, the three conditions being that
>
> a monitored communication from the computer in the predetermined network segment is judged to be infected by the worm at the first judging,
>
> a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging, and

> a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging
>
> (Underlining added for emphasis)

Hence, the above-noted features of claim 5 are a distinction over Spiegel.

The noted features also are a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted features.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 5 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 5.

INDEPENDENT CLAIM 18

As an example, independent claim 18 recites (among other things) the following features:

> the judging unit judges at the second time that a plurality of computers in the predetermined network segment are infected by the worm when all three conditions are satisfied, the three conditions being that
>
> a monitored communication from the computer in the predetermined network segment is judged at the first time to be infected by the worm,
>
> a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged at the first time to be infected by the worm, and
>
> a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination

> addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged at the first time to be infected by the worm

As will be explained below, at least the above-noted features of claim 18 are a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses at column 5, lines 8-10, column 5, lines 47-50, column 6, lines 15-22 and column 3, lines 20-27, "... the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time. ...", "... the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address. ...", "... an embodiment of the WDS 100 ..." and "... If infected, a process 20 is likely to produce a relatively large number of connection attempts to remote destination addresses over a given period of time. ...", respectively.

Spiegel also discloses at column 1, lines 50-60, column 1, lines 60-67, column 3, line 63 to column 4, line 9, "... a network monitoring module (110) observes (205) failed network connection attempts from multiple sources (10,20). ...", "... this determination is based on a set of threshold criteria. ..." and the following, respectively.

> ... the threshold criteria include any one or a combination of the following metrics: (1) the number of failed network connection attempts; (2) the diversity of destination network addresses associated with the failed network connection attempts; (3) the randomness of the failed addresses; and (4) a weighting for each failed network connection attempt according to an attribute thereof (e.g., source or destination address)

However, Spiegel fails to disclose or suggest the following:

> the second judging includes judging that a plurality of the judging unit judges at the second time that a plurality of computers in the predetermined network segment are infected by the worm <u>when all three conditions are satisfied</u>, the three conditions being that

> a monitored communication from the computer in the predetermined network segment is judged at the first time to be infected by the worm,
>
> a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged at the first time to be infected by the worm, and
>
> a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged at the first time to be infected by the worm

(Underlining added for emphasis)

Hence, the above-noted features of claim 18 are a distinction over Spiegel.

The noted features also are a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted features.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 18 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 18.

INDEPENDENT CLAIM 8

As an example, independent claim 8 recites (among other things) the following feature:

> the judging includes identifying a type of the worm executing the monitored communication by comparing features of the monitored communication with features of a communication executed by a worm that are recorded in advance

As will be explained below, at least the above-noted feature of claim 8 is a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses at column 3, lines 58-67, column 6, lines 15-22 and column 5, lines 8-15, "... the heuristic is implemented with a set of threshold criteria that embodies whether the failed connection attempts associated with a source are non-normal. ...", "... an embodiment of the WDS 100 ..." and the following, respectively.

> ... the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time. These collected data are taken and defined as typical failure rates for normal operating conditions. ...

However, Spiegel fails to disclose or suggest the following:

> the judging includes identifying <u>a type of the worm executing the monitored communication</u> by comparing features of the monitored communication with features of a communication executed by a worm that are recorded in advance

(<u>Underlining</u> added for emphasis)

Hence, the above-noted feature of claim 8 is a distinction over Spiegel.

The noted feature also is a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 8 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 8. Claim 43 depends from claim 8, and so at least similarly distinguishes over the asserted combination of references.

<u>INDEPENDENT CLAIMS 22 AND 23</u>

As an example, independent claims 22 and 23 each recite (among other things) the following feature:

> the extracting includes summing up a number of the communication packets for each port number, the communication packets being transmitted in the monitored communication being executed by the worm, and extracting as the reference information, a most frequently appeared port number of the communication packets transmitted in the monitored communication being executed by the worm.

As will be explained below, at least the above-noted feature of claims 22 and 23 is a distinction over Willebeek-LeMair, and thus over its combination with Spiegel.

Willebeek-LeMair discloses the following at paragraph [0031], lines 5-14.

> the extraction of packet features may comprise features 38(1) from the header portion 34 (such as, for example, destination and source IP address, destination and source ports, and the like)

However, Willebeek-LeMair fails to disclose or suggest the following:

> the extracting includes summing up a number of the communication packets for each port number, the communication packets being transmitted in the monitored communication being executed by the worm, and extracting as the reference information, a most frequently appeared port number of the communication packets transmitted in the monitored communication being executed by the worm.

(underlining added for emphasis)

Hence, the above-noted feature of claims 22 and 23 is a distinction over Willebeek-LeMair.

The noted feature also is a distinction over Spiegel as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the

claimed invention. In view of the distinction of claims 22 and 23 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claims 22 and 23.

INDEPENDENT CLAIM 24

As an example, independent claim 24 recites (among other things) the following feature:

> the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the monitored communication being executed by the worm, and extracts, as the reference information, a most frequently appeared port number of the communication packets transmitted in the monitored communication being executed by the worm.

As will be explained below, at least the above-noted feature of claim 24 is a distinction over Willebeek-LeMair, and thus over its combination with Spiegel.

Willebeek-LeMair discloses the following at paragraph [0031], lines 5-14.

> the extraction of packet features may comprise features 38(1) from the header portion 34 (such as, for example, destination and source IP address, destination and source ports, and the like)

However, Willebeek-LeMair fails to disclose or suggest the following:

> the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the monitored communication being executed by the worm, and extracts, as the reference information, a most frequently appeared port number of the communication packets transmitted in the monitored communication being executed by the worm.

(underlining added for emphasis)

Hence, the above-noted feature of claim 24 is a distinction over Willebeek-LeMair.

The noted feature also is a distinction over Spiegel as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 24 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 24.

INDEPENDENT CLAIM 34

As an example, independent claim 34 recites (among other things) the following feature:

> the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the monitored communication being executed by the worm, and extracts, as the reference information, a most frequently appearing port number of the communication packets transmitted in the monitored communication being executed by the worm.

As will be explained below, at least the above-noted feature of claim 34 is a distinction over Willebeek-LeMair, and thus over its combination with Spiegel.

Willebeek-LeMair discloses the following at paragraph [0031], lines 5-14.

> the extraction of packet features may comprise features 38(1) from the header portion 34 (such as, for example, destination and source IP address, destination and source ports, and the like)

However, Willebeek-LeMair fails to disclose or suggest the following:

> the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the monitored communication being executed by the worm, and extracts, as the reference information, a most frequently appearing port number of the communication packets

> transmitted in the monitored communication being executed by the worm.

(underlining added for emphasis)

Hence, the above-noted feature of claim 34 is a distinction over Willebeek-LeMair.

The noted feature also is a distinction over Spiegel as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 34 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 34.

INDEPENDENT CLAIMS 25 AND 27

As an example, independent claims 25 and 27 each recite (among other things) the following feature:

> the extracting further includes summing up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the monitored communication being executed by the worm, and extracting, as the reference information, a direction of the monitored communication wherein the number of the communication packets is over a threshold value.

(Please note that the Office Action refers to wrong recitation as shown below, which was not recited in claims 25 and 27 in the last Response.)

> extracting further includes summing up, for each type of the communication, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference

> information, a type of the communication, the number of the communication packets is over a threshold value

As will be explained below, at least the feature of claims 25 and 27 is a distinction over Bunker, and thus over its combination with Spiegel and Willebeek-LeMair.

Bunker discloses at paragraph [0189], lines 1-11, paragraph [0215], lines 1-5 and paragraph [0220], lines 8-12, "The format of an Enterprise-Wide Summary report includes number of hosts tested; number of new hosts appearing on network; ..." and the following, respectively.

> Vulnerability Trending shows total counts of vulnerabilities as well as counts grouped by risk level. Summary graphical information depicts severity, likely impact, skill level needed to exploit, and likely cause of vulnerabilities

> ... The Standard Report shows vulnerability trending showing total counts of vulnerabilities as well as counts grouped by risk level; fix reports showing count of vulnerabilities corrected vs. those left unresolved as well as a risk level of fixed and unfixed vulnerabilities; ...

However, Bunker fails to disclose or suggest the following:

> the extracting further includes <u>summing up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the monitored communication being executed by the worm</u>, and extracting, as the reference information, a direction of the monitored communication wherein the number of the communication packets is over a threshold value.

(<u>underlining</u> added for emphasis)

Hence, the above-noted feature of claims 25 and 27 is a distinction over Bunker.

The noted feature also is a distinction over Spiegel and Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel and Willebeek-LeMair as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claims 25 and 27 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claims 25 and 27.

INDEPENDENT CLAIM 28

As an example, independent claim 28 recites (among other things) the following feature:

> the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the monitored communication being executed by the worm, and extracts, as the reference information, a direction of the monitored communication wherein the number of the communication packets is over a threshold value.

(Please note that the Office Action refers to wrong recitation as shown below, which was not recited in claim 25 or 27 in the last Response.)

> extracting further includes summing up, for each type of the communication, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a type of the communication, the number of the communication packets is over a threshold value

As will be explained below, at least the above-noted feature of claim 28 is a distinction over Bunker, and thus over its combination with Spiegel and Willebeek-LeMair.

Bunker discloses at paragraph [0189], lines 1-11, paragraph [0215], lines 1-5 and paragraph [0220], lines 8-12, "The format of an Enterprise-Wide Summary report includes number of hosts tested; number of new hosts appearing on network; ..." and the following, respectively.

> Vulnerability Trending shows total counts of vulnerabilities as well as counts grouped by risk level. Summary graphical information depicts severity, likely impact, skill level needed to exploit, and likely cause of vulnerabilities
>
> ... The Standard Report shows vulnerability trending showing total counts of vulnerabilities as well as counts grouped by risk level; fix reports showing count of vulnerabilities corrected vs. those left unresolved as well as a risk level of fixed and unfixed vulnerabilities; ...

However, Bunker fails to disclose or suggest the following:

> the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the monitored communication being executed by the worm, and extracts, as the reference information, a direction of the monitored communication wherein the number of the communication packets is over a threshold value.

(underlining added for emphasis)

Hence, the above-noted feature of claim 28 is a distinction over Bunker.

The noted feature also is a distinction over Spiegel and Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel and Willebeek-LeMair as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 28 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 28.

INDEPENDENT CLAIM 35

As an example, independent claim 35 recites (among other things) the following feature:

> the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the monitored communication being executed by the worm, and extracts, as the reference information, a direction of the monitored communication wherein the number of the communication packets is over a threshold value.

(Please note that the Office Action refers to wrong recitation as shown below, which was not recited in claim 25 or 27 in the last Response.)

> extracting further includes summing up, for each type of the communication, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a type of the communication, the number of the communication packets is over a threshold value

As will be explained below, at least the feature of claim 35 is a distinction over Bunker, and thus over its combination with Spiegel and Willebeek-LeMair.

Bunker discloses at paragraph [0189], lines 1-11, paragraph [0215], lines 1-5 and paragraph [0220], lines 8-12, "The format of an Enterprise-Wide Summary report includes number of hosts tested; number of new hosts appearing on network; ..." and the following, respectively.

> Vulnerability Trending shows total counts of vulnerabilities as well as counts grouped by risk level. Summary graphical information depicts severity, likely impact, skill level needed to exploit, and likely cause of vulnerabilities
>
> ... The Standard Report shows vulnerability trending showing total counts of vulnerabilities as well as counts grouped by risk level; fix reports showing count of vulnerabilities corrected vs. those left unresolved as well as a risk level of fixed and unfixed vulnerabilities; ...

However, Bunker fails to disclose or suggest the following:

> the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the monitored communication being executed by the worm, and extracts, as the reference information, a direction of the monitored communication wherein the number of the communication packets is over a threshold value.

(underlining added for emphasis)

Hence, the above-noted feature of claim 35 is a distinction over Bunker.

The noted feature also is a distinction over Spiegel and Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel and Willebeek-LeMair as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 35 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 35.

In view of the foregoing discussion, the rejection of claims 1, 3-5, 8, 13, 15-18, 22-25, 27, 28, 34, 35, 41 and 43 is improper. Accordingly, withdrawal of the rejection is respectfully requested.

Conclusion

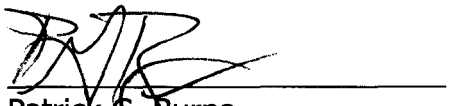
In light of the foregoing, withdrawal of the rejections of record and allowance of this application are earnestly solicited.

Should the Examiner believe that a telephone conference with the undersigned would assist in resolving any issues pertaining to the allowability of the above-identified application, please contact the undersigned at the telephone number listed below.

Please grant any required extensions of time and charge any fees due in connection with this request to deposit account no. 07-2069.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By 

Patrick G. Burns
Registration No. 29,367

July 19, 2010

300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
(312) 360-0080

Customer No. 24978